

Fig. 1

System Console Devices (PCs)

Fig. 2

Computer System  
(or Server)

207A



Device ID and  
shared secret  
stored on  
hard drive

203  
Local Connection  
209

207B



207C



Device ID and  
shared secret  
stored in  
security chip on  
PC's system  
board

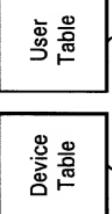


204A



Device ID and  
shared secret  
stored in  
smart card

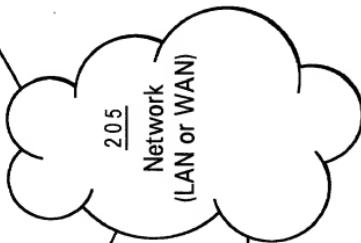
2/9

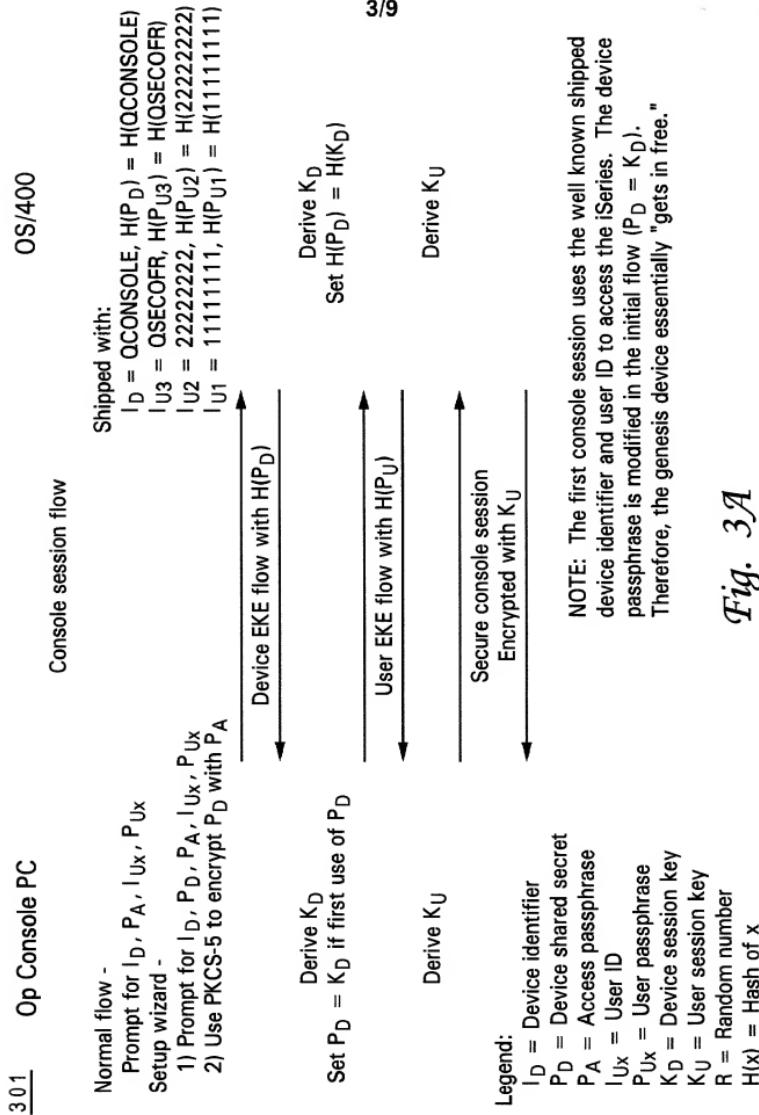
Console Control  
Program

204B

204C

205  
Network  
(LAN or WAN)





303

- Generate DH parameters g and p
- Where g = base; p = prime; these values do not have to be secret (public-info)
- Make g and p constants in server and client EKE code

Client EKE

Make g, p constants

Generate R and do DH Phase 1

Send --&gt;

Device ID,  $H(P_D)[\text{public-info}]$ 

*Fig. 3B*

Server EKE

- Make g, p constants

Generate R and do DH Phase 1

Generate challenge B

Derive K from DH Phase 2

<-- Send (Phase 1 public-info)

Derive K from DH Phase 2

Generate challenge A

Send --&gt;

 $K[\text{challenge A, challenge B}]$ 

Authenticate user A

<-- Send

 $K[H(\text{challenge A, challenge B})]$ 

Authenticate server B

Refer to BSAFE Reference Manual for description of DH Phase 1 &amp; 2.

NOTE: The challenge strings must be a different length than the encryption block.

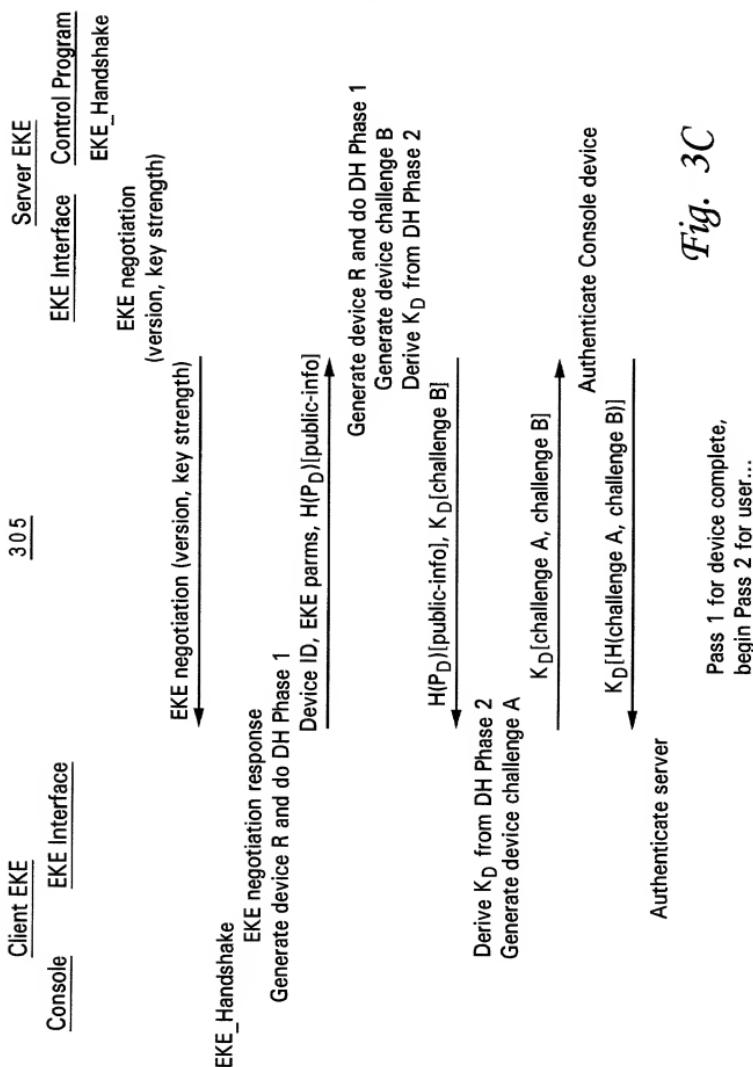
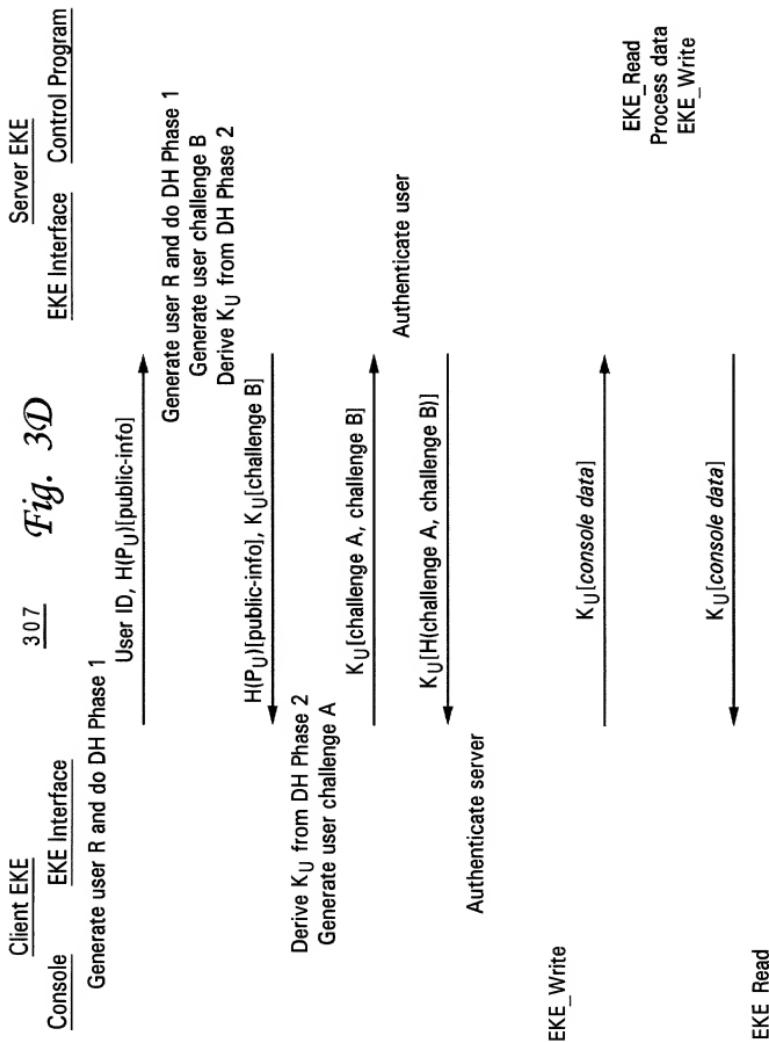


Fig. 3C



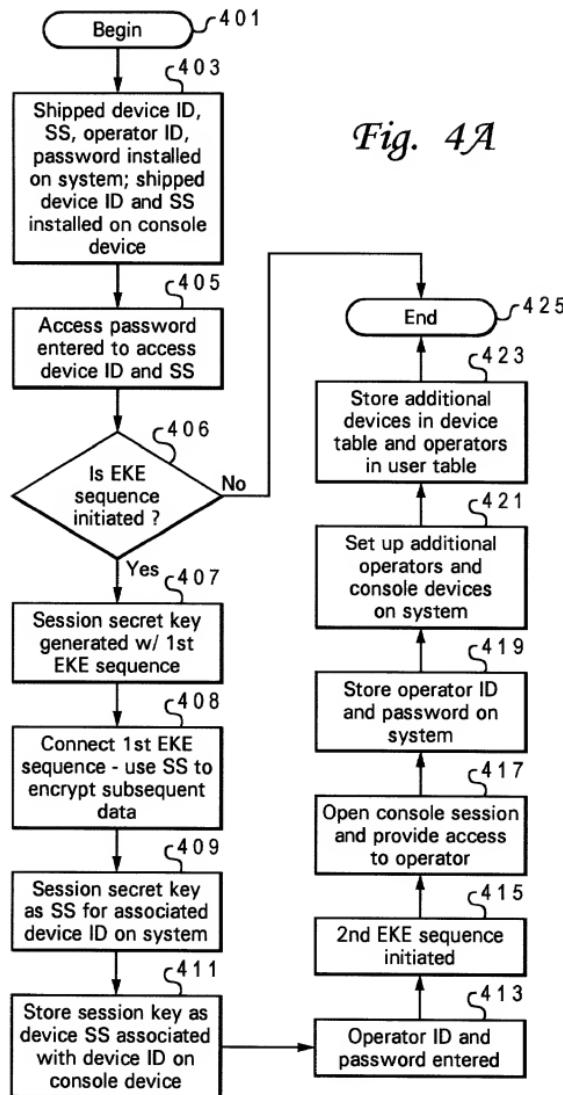


Fig. 4A

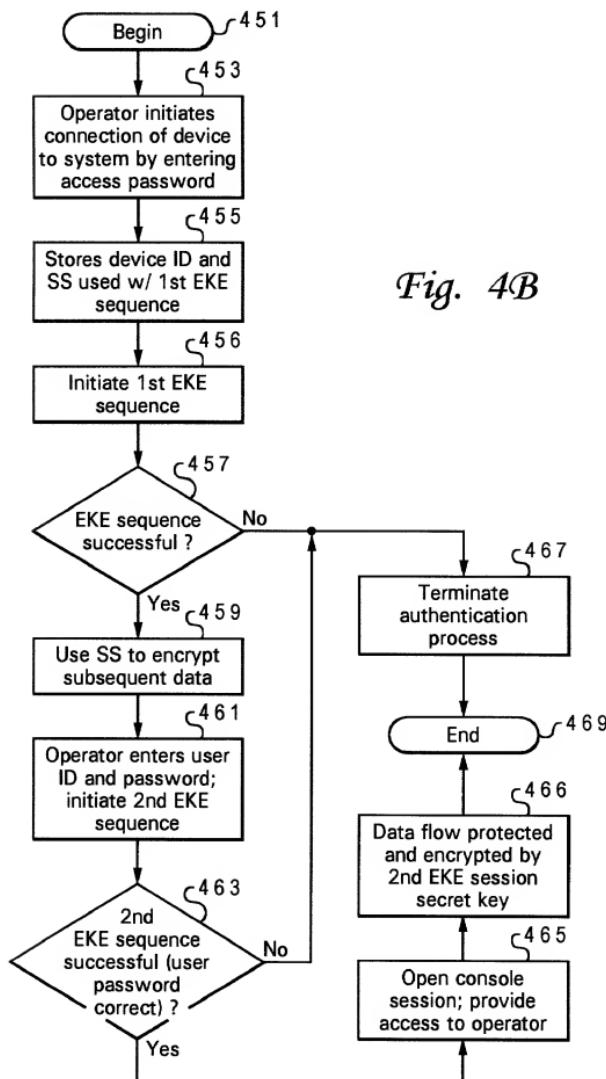


Fig. 4B

T00E20 "84582860

Server	
Device Table $\hookrightarrow$	
Device Identifier	Hashed shared secret
QCONSOLE	H(shared secret)
DEVICE2	H(shared secret)

User Table $\hookrightarrow$	
User Identifier	Hashed password
11111111	H(password)
22222222	H(password)
QSRV	H(password)
QSECOFR	H(password)

Fig. 5B

Client Device (PC) $\hookrightarrow$	
Server Connection	Hash (device identifier, shared secret)
Server1	Hash (device identifier, shared secret)
Server2	Hash (device identifier, shared secret)

Fig. 5A